1. A method for controlling disclosure of sensitive information provided by an information provider, comprising the steps of:

obtaining at least one disclosure condition;

hiding copies of the sensitive information in a network at locations not disclosed to the information provider;

checking at least once for occurrence of the disclosure condition; and

if occurrence of the disclosure condition is detected then disclosing at least a portion of the sensitive information.

2. The method of claim 1, wherein the sensitive information is hidden by encryption.

3. The method of claim 1, wherein the sensitive information is hidden by a file disguise.

4. The method of claim 1, wherein the hiding step hides at least ten copies of the sensitive information.

5. The method of claim 1, wherein the hiding step hides at least one hundred copies of the sensitive information.

6. The method of claim 1, wherein the hiding step hides at least one thousand copies of the sensitive information.

7. The method of claim 1, wherein the hiding step creates at least one roving message copy.

8. The method of claim 1, wherein the hiding step creates at least one poised message copy.

9. The method of claim 1, further comprising the steps of:

obtaining at least one deletion condition;

checking at least once for occurrence of the deletion condition; and

if occurrence of the deletion condition is detected then deleting at least a portion of the sensitive information.

10. The method of claim 9, wherein cancellation by the information provider is a deletion condition, and the user requests such cancellation.

11. The method of claim 1, further comprising the steps of accepting a message update and storing the message update.

12. The method of claim 1, wherein the message update is a searching update which is not directed at a particular copy of the corresponding message to be updated.

13. The method of claim 1, wherein the message update is directed at a particular copy of a corresponding roving message to be updated.

14. The method of claim 1, wherein the message update is directed at a particular copy of a corresponding poised message to be updated.

15. The method of claim 1, wherein at least a portion of the sensitive information is disclosed using at least one destination specified by the information provider.

16. The method of claim 15, wherein a region destination was specified by the information provider and disclosure includes disclosure in that region.

17. The method of claim 15, wherein a deadman switch disclosure condition was specified by the information provider and disclosure is triggered by that condition.

18. The method of claim 1, wherein at least a portion of the sensitive information is disclosed using at least one format specified by the information provider.

19. A computer system comprising a network, message storage means for storing in the network copies of a message, and message disclosure means for disclosing the message if a predefined condition is detected.

20. The system of claim 19, wherein the message storage means comprises an encryption means for encrypting at least one message component.

21. The system of claim 19, wherein the message storage means comprises a digital signature means for digitally signing at least one message component.

22. The system of claim 19, wherein the message storage means comprises code to send a notice to a specified email address after the message has been stored.

23. The system of claim 19, wherein the message disclosure means comprises an email message generator for creating and mailing at least one email message containing a copy of at least a portion of the stored message.

24. The system of claim 19, wherein the message disclosure means comprises a web page generator for creating and posting at least a portion of a web page containing a copy of at least a portion of the stored message.

25. The system of claim 19, wherein the message disclosure means comprises code for detecting a deadman switch for triggering disclosure.

26. The system of claim 19, wherein the message disclosure means comprises code for detecting a reverse deadman switch for triggering disclosure.

27. The system of claim 19, wherein the network includes a local area network.

28. The system of claim 19, wherein the network includes a geographically dispersed network and at least two copies of the message are geographically dispersed in the network.

29. The system of claim 19, wherein the network includes nodes on different continents and at least two copies of the message are stored on different continents in the network.

30. The system of claim 19, further comprising a means for changing the location of message copies.

31. The system of claim 19, further comprising a means for placing message copies in at least one file disguise.

32. The system of claim 19, further comprising a message deletion means for deleting message copies.

33. The system of claim 32, wherein the message deletion means comprises a means for performing an emergency action in response to an apparent deletion request.

34. The system of claim 32, wherein the message deletion means comprises a cancellation means for deleting all stored message copies.

35. The system of claim 34, wherein the cancellation means requires authentication information which confirms that the source of the cancellation request is the same as the source of the message to be canceled.

36. The system of claim 19, further comprising a message update storage means for storing message updates.

37. The system of claim 36, wherein the message update storage means comprises code for creating decoy updates.

38. The system of claim 36, wherein the message update storage means comprises code for creating at least one secrecy renewal.

39. The system of claim 36, wherein the message update storage means comprises code for creating at least one address marker.

40. The system of claim 36, wherein the message update storage means comprises code for creating at least one searching update.

41. The system of claim 36, wherein the message update storage means comprises code for creating at least one update to a roving message.

42. The system of claim 36, wherein the message update storage means comprises code for creating at least one update to a poised message.

43. A signal embodied in a network for controlled message disclosure, the signal comprising a sensitive information component and a disclosure condition component.

44. The signal of claim 43, wherein at least the sensitive information component is encrypted.

45. The signal of claim 43, wherein at least the sensitive information component is compressed.

46. The signal of claim 43, wherein at least the sensitive information component is digitally signed.

47. The signal of claim 43, further comprising a destination component.

48. The signal of claim 43, further comprising a disclosure format component.

49. The signal of claim 43, further comprising an identification component.

50. The signal of claim 43, further comprising a traveling program component.

51. The signal of claim 43, further comprising a deletion condition component.

52. The signal of claim 43, further comprising code for monitoring conditions to determine if disclosure or deletion is appropriate.

53. The signal of claim 52, wherein the code operates independently of any message update signals.

54. A computer storage medium having a configuration that represents data and instructions which will cause at least a portion of a computer system to perform method steps for controlled message disclosure, the method steps comprising the steps of:

obtaining at least one disclosure condition;

storing copies of a message in a network;

checking for occurrence of the disclosure condition; and

if occurrence of the disclosure condition is detected then disclosing at least a portion of the message.

55. The storage medium of claim 54, wherein the storing step comprises placing a copy of the message in a file disguise.

56. The storage medium of claim 54, wherein the storing step stores at least one thousand copies of the message.

57. The storage medium of claim 54, wherein the storing step stores at least one roving message copy.

58. The storage medium of claim 54, wherein the storing step stores at least one poised message copy.

59. The storage medium of claim 54, wherein the method further comprises the steps of:

obtaining at least one deletion condition;

checking for occurrence of the deletion condition; and

if occurrence of the deletion condition is detected then locating copies of the message and deleting all located copies of the message.

60. The storage medium of claim 54, wherein the method further comprises the steps of accepting a message update and storing the message update.

61. The storage medium of claim 54, wherein at least a portion of the message is disclosed to at least one destination.

62. The storage medium of claim 61, wherein disclosure includes sending a copy of at least a sensitive information component of the message to an email destination.